Responsibility Modelling for Civil Emergency Planning

Ian Sommerville, Tim Storer and Russell Lock

School of Computer Science, North Haugh, St Andrews, Fife, Scotland, KY16 9SX

Abstract

This paper presents a new approach to analysing and understanding civil emergency planning based on the notion of responsibility modelling combined with HAZOPS analysis of information requirements. Our goal is to represent complex contingency plans so that they can be more readily understood, so that inconsistencies can be highlighted and vulnerabilities discovered. In this paper, we outline the framework for contingency planning in the UK and introduce the notion of responsibility models as a means of representing the key features of contingency plans. Using a case study of a flooding emergency, we illustrate our approach to responsibility modelling and suggest how it adds value to current textual contingency plans. We briefly describe CASE tool support that we are developing for building and analysing responsibility models and discuss future directions for this research.

Key words: contingency planning, responsibility modelling, socio-technical systems

1 Introduction

The management of large scale emergencies is a complex activity. There are a diverse range of possible emergency scenarios, including terrorist attacks and serious accidents, environmental emergencies, such as flooding, and the outbreak of animal and human diseases. Responding to these emergencies involves many different organisations, including the emergency services (fire, police, ambulance), local authorities, environmental agencies and charities.

Email address: {ifs, tws, rl}@cs.st-andrews.ac.uk (Ian Sommerville, Tim Storer and Russell Lock).

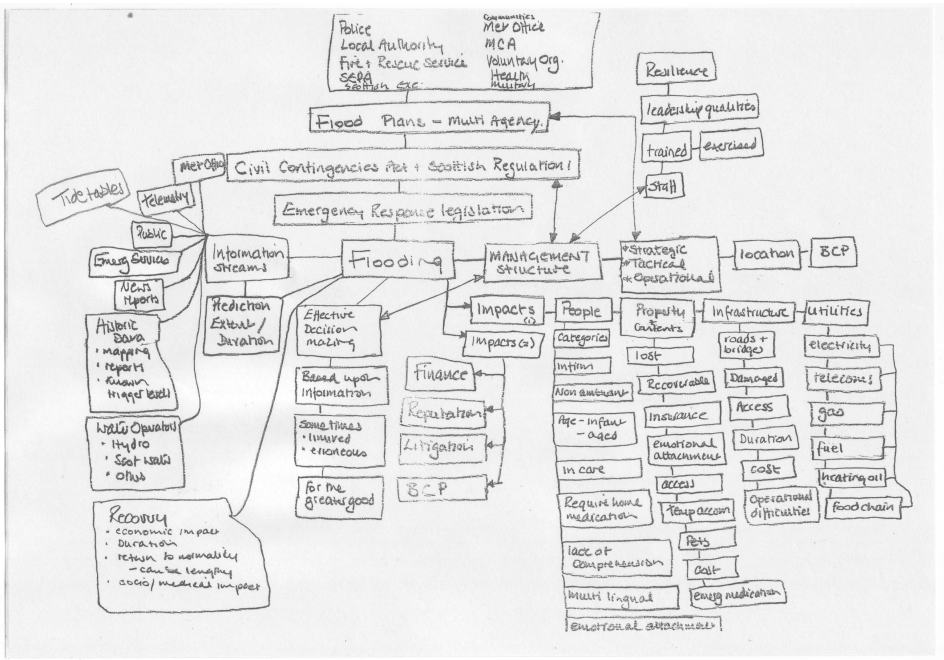


Fig. 1. Some issues to be considered during the response to a flooding event. The sketch was by an Emergency Planning Officer, during early discussions of this work.

Civil emergency (or contingency) planning is concerned with drawing up plans to cope with these scenarios. The process is one of several aspects of the broader activity of crisis management within organisations [22]. As well as the task of dealing with immediate problems, planners must take into account issues such as the displacement of people, dealing with the media and managing and maintaining the emergency team over perhaps several days of work. Figure 1 is a sketch of *some* of the issues that an emergency planner discussed with us when explaining the response to a flooding event, a particular concern in the United Kingdom, due to a series of unexpectedly severe weather events [10,19].

From a single organisational perspective, the purpose of planning is to provide guidance on the procedures, resources and training that are likely to be required for a particular emergency. Inter-organisational contingency plans are used by individual agencies to understand both the responsibilities they hold and the responsibilities that others can be expected to discharge. Effective communications and information exchange between organisations is essential for the effective management of emergencies. Thus, contingency planning should consider inter-organisational information and communication requirements.

The inherently unpredictable nature of emergencies is such that it makes little sense to express contingency plans in terms of detailed processes and actions [22,20]. Rather, these plans set out what is expected in particular situations, the agencies that will be involved and the assumptions that are made. These

assumptions generally include what is expected of different agencies who cooperate to manage the emergency. Often, plans are written in terms of assumed responsibilities. For example, they may set out that it is the responsibility of a meteorological agency to provide information concerning rainfall; that an environment agency is responsible for using the information to predict potential flooding patterns; that the police are responsible for evacuating residents from an area in danger; and that the responsibility of a local authority to provide shelter for evacuees.

The contingency plans we have reviewed are predominantly textual documents with informal diagrams and tables. As with all complex documents, there is scope for error, omission, ambiguity and misunderstanding. Smith has also noted that contingency plans often contain assumptions which are later exposed as invalid during an exercise or actual crisis [21]. These problems are sometimes concealed by the free text nature of documents and, as is always the case in large texts, extracting the key points requires a great deal of work on the part of the reader. This paper argues that the development of supplementary graphical notations is useful in expressing the key issues and points in the plan in a way that is more immediate than paragraphs of text, and in providing a basis for questioning the assumptions embedded in plans .

The complex relationships which are developed between organisations during contingency planning suggested to us that techniques previously used for the analysis of large scale complex socio-technical systems may successfully be applied to this area. In particular, this paper focuses on analysis of contingency planning from the perspective of responsibilities. The paper proposes that *responsibility modelling* can be effectively employed to model and analyse the responsibilities that may need to be discharged during a response to a civil emergency.

A responsibility model is a way of representing the responsibilities of the agents and agencies involved in handling a civil emergency, the resources required to discharge these responsibilities and some of the relations that exist between responsibilities, agents and resources. We argue that responsibility modelling provides an appropriate abstraction for modelling contingency plans, since such documents are often written in terms of the responsibilities held by responder organisations. Contingency plans cannot provide a detailed explanation of the process by which an emergency will be managed, given the complexity and unpredictability of such events. Responsibility modelling can instead be used as a mechanism to abstract over details that cannot or do not need to be specified in an overall plan. In addition, the evolving nature of contingency planning can be supported by the analysis of plan documents from the perspectives of responsibilities to identify potential vulnerabilities that may compromise the success of the emergency response.

Responsibility models are not simply adjuncts to a textual contingency plan that provide a summary of key points of the plan. We argue that they can be used in several different ways [11]:

(1) As a means of supporting discussion about systems that cross organisational boundaries. Responsibility misunderstandings in such situations are common and by making responsibilities explicit there is the potential to expose such misunderstandings [16].
(2) As a means of identifying vulnerabilities in a system expressed in terms of the potential for responsibility failure. Responsibility failure occurs when an agent does not discharge a responsibility as expected by other agents in the system. This may occur, for example, due to a mis-understanding when an agent does not know it is expected by other agents to discharge a responsibility [23].
(3) As a means of helping to identify information requirements and vulnerabilities. The discharge of a responsibility often requires information to be available to the agent assigned that responsibility. Responsibility models can help identify what information is required, where it comes from and what problems occur if it is unavailable, incomplete or incorrect.
(4) As a means of conceptual system modelling [23]. When attempting to understand and explain complex socio-technical systems, it may be helpful to create a conceptual system model in terms of the responsibilities in that system.

Different types of agent (both technical and human) generally contribute to the dependability of systems in different ways. For example, technical components can perform repetitive tasks without error, human operators, with their greater flexibility can often deal with unplanned situations before failures become observable to those interacting with a given system. Given that both types of system entity are responsible for contributing to the overall dependability of a system, this paper will argue that an analysis of how responsibility for dependability is distributed throughout a system provides an insight into potential vulnerabilities of the system. For example, analysis of a given responsibility model may show how the allocation of a responsibility to only one agent could create a central point of failure in a responsibility structure; or identify where a responsibility has been inappropriately delegated to an unqualified agent.

This paper sets out our approach to responsibility modelling and illustrates, by example, how responsibility models can be useful in planning for civil contingencies. Section 2 presents an outline of the process of contingency planning. Section 3 examines related work on the use of responsibility modelling for the analysis of socio-technical systems. Section 4 presents the conceptual basis for the responsibility models used in this paper whilst Section 5, the case study, presents a selection of examples of responsibility models constructed

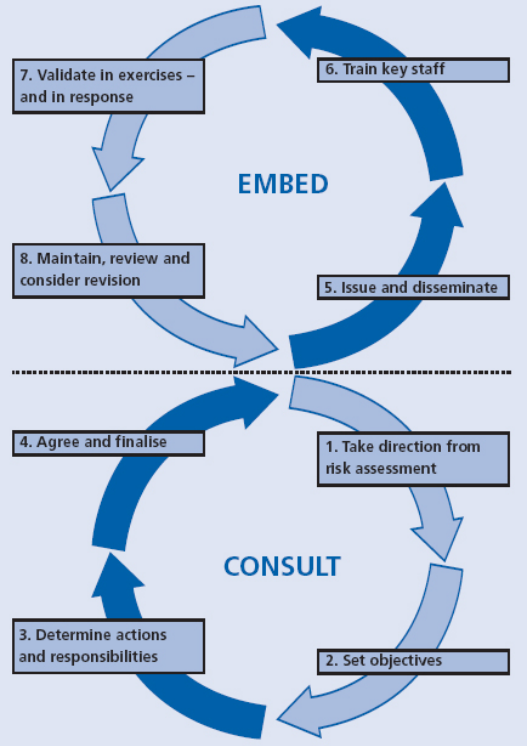


Fig. 2. The emergency planning cycle, extracted from [14]. The cycle consists of two major processes; consultation and implementation.

from a real world contingency plan. Finally, Section 6 summarises the work and considers areas of future research.

2 Contingency Planning

The process of preparing and planning for a civil emergency in the UK is illustrated in Figure 2, extracted from the UK government's guidance on the Civil Contingencies Act 2004 [5,14]. Contingency planning is a cyclic activity, divided into two major processes.

For the consultation phase it is first necessary to identify the emergency scenarios that are of interest. Emergency scenario selection is informed by the risk assessment process, which identifies vulnerabilities in civil infrastructure. However, it should be noted that the criteria for selecting scenarios, the next stage of planning, are not necessarily based on the severity or expected frequency of an incident, but may also be politically motivated. For example, planning for the provision of fallout shelters during the Cold War was motivated largely by political considerations, as the probability of use was relatively low, the envisaged costs considerable, and the end benefits difficult to quantify [27].

Before plans can be established for a specific emergency scenario, it is first necessary to consult with the organisations which would be involved in the response to an incident. In the United Kingdom, response organisations are coordinated by Civil Resilience Forums, which provide an administrative basis for contingency planning across organisations. The outcome of the consultation process is a set of responsibilities assigned to different agencies in the event of an incident. It is important to note that the contingency planning process brings together organisations with potentially conflicting objectives. Efforts toward providing greater clarity in the contingency planning process are beneficial, for example, in preventing misunderstandings during an emergency response.

During the Embedding phase the outline plan is disseminated to relevant organisations for information and to assess the appropriateness of the plan for each organisational domain. Appropriate training can then be planned and undertaken. The robustness of an emergency plan and the training provided to personnel is frequently evaluated using emergency exercises. Such exercises may be "table top", i.e. largely simulated, or larger scale live exercises with appropriate deployment of resources to test the speed of response, reliability of communications infrastructure and so on. The use of exercises of this type is widespread, with UK government policy stating that exercises should take place for each scenario emergency plan on a regular basis. Exercises are designed to test the resilience of a given emergency plan and often lead to substantive changes . It should be noted that this is not necessarily recognition of flaws in the original plans, rather that the assumptions on which the original plan were written no longer hold.

3 Background

The notion of 'responsibility' is one that is widely used in everyday discourse but it is surprisingly difficult to establish a precise definition of the term. For the purposes of the work described here, we have established the following definition:

> *A duty, held by some agent, to achieve, maintain or avoid some given state, subject to conformance with organisational, social and cultural norms.*

The term 'duty' refers to more than simply a statement that a given task should be completed, it also encompasses aspects of accountability. It is important to note that failure to fulfill a given duty could in fact be due to circumstances beyond the control of the agent in question. It does not therefore follow automatically that the agent should be blamed for a given failure.

The terms organisational, social and cultural norms relate to the inherent nature of responsibilities. Responsibilities are rarely broken down to individual instructions (for anything but the most trivial of system this would extremely difficult), instead they represent higher level constructs encompassing a remit for initiative. Initiative is bounded by professional conduct, from an organisational perspective as well as wider social and cultural constraints. For example doctors discharge responsibilities subject to ethical constraints, companies operate subject to the financial regulations of their host country. The notion of a responsibility permits a useful abstraction over this complexity.

Responsibility modelling has been proposed by several authors [2,13,25] as a useful construct for analysing the dependability of socio-technical systems. The work partly originates from the perceived failure of purely technical solutions. A key preliminary to the development of responsibility analysis is the identification of a system as consisting of both technical and social/organisational entities; both of which contribute to the achievement of the overall goals or objectives that are the systems purpose. The term socio-technical system, originating in the field of organisational design, has been adopted by the computer science community, in reference to the interactions that occur between human and organisational agents and software systems [18]. In addition to achieving system goals, both social and technical entities contribute to the broader dependability of a system. The notion that human agents in a system, if employed appropriately, can contribute positively to the dependability of a technical system is one that is often missed in discussions of software dependability [1].

Graphical models of responsibility were first proposed by Blyth et al in the ORDIT methodology [2], a notation for describing the responsibilities that agents hold with respect to one another. Strens, Dobson and Sommerville have argued for the importance of analysing responsibility and the need to view roles with respect to the responsibility relationships they hold [12,13,25]. Dewsbury and Dobson have edited a collection of papers [11] that describe much of the research undertaken on responsibility as part of the DIRC project, [1] presenting analyses of inappropriate responsibility allocation in socio-technical systems. In particular, the work includes an analysis of the Ladbroke Grove rail accident inquiry from a perspective of responsibilities [16]. The work also includes a graphical notation for responsibility by Sommerville. The purpose of the notation is primarily to support the discussion of responsibility allocations during a system development process [23], and in this respect is similar to the approach taken by proponents of the soft systems methodology [6].

Goal based modelling approaches, such as i^* and KAOS are intended to expose high level dependencies between objectives in a given system [9,28]. Sub-goals

[1] `http://www.dirc.ac.uk`

may be derived from higher level objectives and assigned to agents for completion. Goals are achieved through the fulfillment of some or all sub-goals. Relationships between sub-goals express (and, or etc) express the possible ways in which the super-goal may be achieved. Analysis of such models can examine, for example, whether a super-goal may fail due to the failure of a single sub-goal (brittleness), or whether a particular agent has been overloaded with too many goals to achieve.

Despite some similarities, research on responsibility modelling differs from existing goal based techniques. Whilst the notion of responsibility modelling may be viewed as incorporating the specification of objectives to be achieved, there is also an acknowledgment that in complex socio-technical systems, the achievement of an objective (i.e. the discharge of responsibility) is subject to a range of often implicit constraints and that even with the best efforts of an agent, a goal may not be achieved. These constraints are difficult to explore and model using a goal-based approach which focuses principally on what has to be achieved. In contrast to goal based systems, there are circumstances in which an authority may judge that a responsibility has been been appropriately discharged, despite the fact that a goal has not been achieved. The notion of responsibility embodies an embedded assumption that it is how an agent acts and not just what is achieved that is important. In the example given above, a doctor who has carried out the correct procedures may be considered to have successfully discharged their responsibility for patient care, even though a patient dies.

4 Responsibility Models

For the purposes of this paper, a responsibility model is a succinct denotation of the responsibilities involved in handling some civil emergency, the agents or agencies that have been assigned specific responsibilities and the relations between agencies, responsibilities and resources. Construction of responsibility models of contingency plans clarifies the analysis of modelled relationships for their appropriateness - for example, whether an agent has been assigned a reasonable responsibility to discharge.

A recurring theme identified in debrief reports of emergency response exercises are failures related to communication arrangements. Such reports describe how participants did not receive necessary information in order to discharge their responsibilities in a timely fashion, or similarly did not distribute information to others appropriately. Additionally, Smith has noted that seemingly realistic emergency scenarios are often dismissed by organisational management because they are perceived as being either of low probability or prevented from occurring by existing controls [21].

We have therefore designed our modelling notation so that HAZOPS style "what if" risk analysis can also be applied to information resources to present an analysis of a plan's robustness in the event of failure of these resources. HAZOPS methodologies were designed to analyse industrial processes, predominantly in the chemical industry; however they have also been employed for the analysis of information systems for example [4,17], in order to establish the consequences of failure of particular information flows. An advantage of this systematic approach to scenarios is that stakeholders are encouraged to consider the consequences of particular events occurring, even if they are judged to be of low probability. HAZOPS-style analysis is provided as part of the case study examples within this paper, to illustrate the application of this approach.

We have revised the graphical notation proposed by Sommerville as a suite of related graphical viewpoints with a corresponding formal semantics of the model. The views simplify the process of diagram (and hence model) construction by permitting users to concentrate on particular aspects of a responsibility model at a time. In addition, tool support for the notation guides a user between different viewpoints, providing a sense of inter-connection between the different views of responsibility.

This section provides an informal explanation of the underlying model of responsibility adopted for use in the graphical views employed here, for more detail see [24]. The notation described here is a subset of the entities and relationships developed for use in a broader collection of case studies of responsibility modelling.

The model of responsibility presented in this paper is as follows. An *agent* (denoted by a name in angle brackets) may become the holder of a *responsibility*, through an act of *assignment* by another agent, the responsibility *authority* or through organisational custom and practice. Agents may be organisations (denoted by an 'O' over the entity), for example the Fire Service, or individuals (denoted by an 'H' over the entity) for example, Jane Smith. The term assignment here incorporates responsibility transfer (an agent assigns a responsibility to another) and assumption (an agent assigns a responsibility to itself). The representation of an agent assigned a responsibility by an authority is illustrated in Figure 3. The figure denotes the assignment of the responsibility "Maintain the peace" by the agent "Government", to the agent "Police". The Police are the holder of the responsibility (denoted by a line terminated by a square), whilst the Government is the authority (denoted by a line, crossed at termination).

Figure 4 illustrates the use of organisational entities as a means of constructing complex agent structures. Contingency plans often refer to a group of agents as collectively the holders of some responsibility. In the example shown in Figure

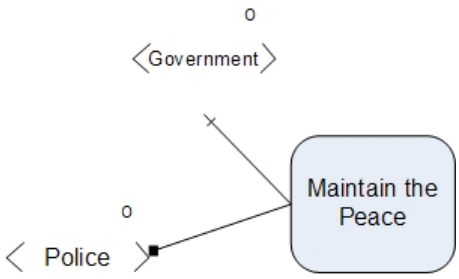


Fig. 3. Responsibility Assignment

4(a), a single organisation, the 'Health Services' is denoted as being responsible for provision of health information, medical care and the instigation of follow up treatments during the recovery phase of a emergency response.

In this example, the notion of a 'Health Services' organisation is an abstraction; in fact the responsibilities are discharged by three 'actual' agencies, the Health Protection Unit, the Primary Care Trust (the organisation responsible for medical services outside of hospitals) and the Hospital Trust (the organisation responsible for all hospitals in a given area). Membership of the 'Health Services' organisation is denoted by a line terminated by a diamond in Figure 4(b). Other agencies using the contingency plan do not need to concern themselves with how these agencies will discharge their responsibilities. Rather, other agencies may use the model to develop more detailed plans of the discharge of their own responsibilities, without concern for the detailed planning by the 'Health Services' organisations.

Thus far, the discussion of the responsibility model has referred to two basic types, responsibilities and agents. However, to provide more detail for responsibility scenarios, we need to introduce the notion of a *resource*. Resources are artifacts in a responsibility model that are used by agents in the discharge of responsibilities. They are categorised as information resources and physical resources. Information resources are used to model the information requirements needed to discharge a responsibility, such as an evacuation priority list. Physical resources refer to artifacts employed by an agent in order to discharge their responsibility, portable flood barriers, for example.

5 Case Study

To illustrate the approach that we have developed, this section presents a case study which illustrates the use of responsibility modelling as a tool for the reliability analysis of a contingency plan. The work presented in this case study is an illustrative analysis constructed on the basis of written documents. It highlights the benefits of our approach and we think could act as the basis for

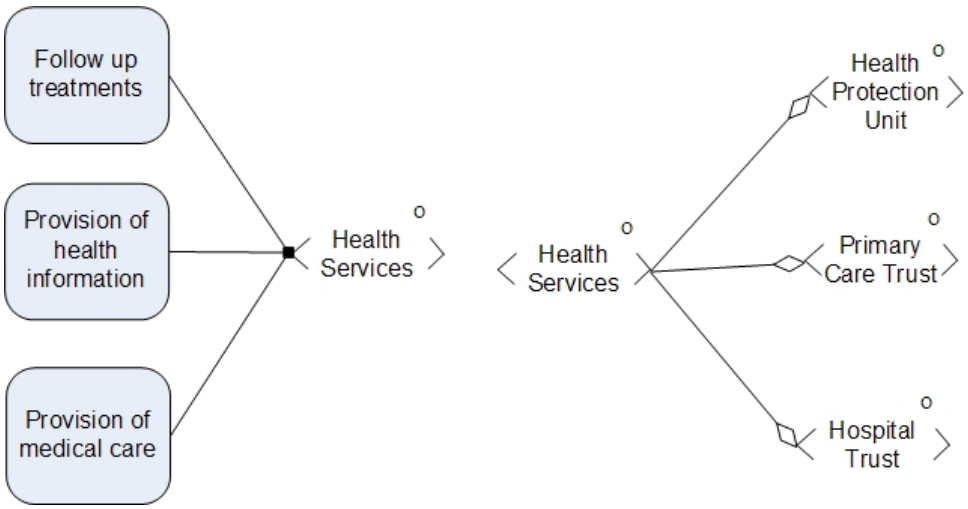


Fig. 4. 'Health Services' responsibilities and organisational membership. Figure 4(a) illustrates the responsibilities of the 'Health Services' organisation, a construct used in the contingency plan to describe a collection of medical-related agencies. Figure 4(b) illustrates the membership of the 'Healh Services organisation from the perspective of the revised flood plan.

stimulating discussions about the information and assumptions in the plan. We do not claim that the case study demonstrates vulnerabilities that still exist within a prepared response to flooding.

The responsibility modelling notation described above is used to document examples of responsibility assignment from the contingency plan. The purpose of the modelling is to represent the salient parts of contingency plans in an easily readable format, and to provide a framework for questioning these plans to identify possible errors and omissions. Thus, we believe, we can avoid system problems and failures when an emergency occurs which affect the dependability of the overall socio-technical system.

The responsibility models are derived from a collection of documents related to the storms and associated flooding in January 2005 which occurred in Carlisle, a city in the north of England. We have used several documents including: the Cumbria County Council General Emergency Plan [7], which was the initial contingency plan upon which the emergency response to the floods was based; the debriefing report for the storms, which reviewed the performance of the plan in retrospect of the emergency [10]; and the Cumbria County Council flood plan, which was developed following the floods of 2005 [8].

The models presented illustrate particular examples from the debrief report where the mis-understanding or mis-assignment of responsibilities in the plan caused difficulties during the response. The models are also used as a basis for conducting a HAZOPS-style analysis of information resources which are

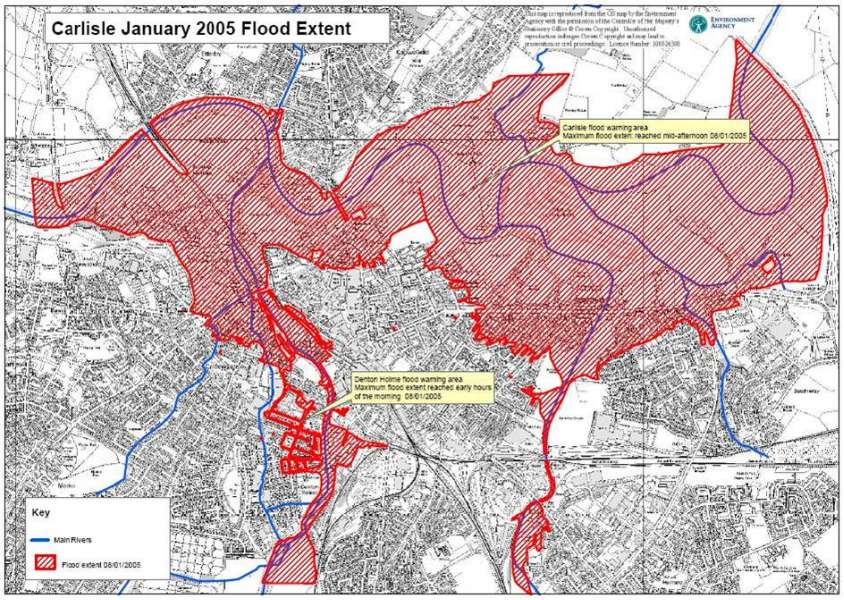


Fig. 5. Extent of floods around Carlisle, Cumbria January 2005. Source: [10].

likely to be needed to discharge a responsibility, and assesses the likelihood and consequences of the information's unavailability.

5.1 Background

Between 7th and 8th of January 2005, the north west of England and, in particular, the city of Carlisle suffered substantial flooding due to heavy rainfall. The flooding was a combination of the heavy rainfall and the blocking of drainage channels by debris caused by the storms. In addition to the flooding, the severe storms caused structural damage to buildings, and caused 24 large vehicles to be blown over, blocking major access roads. The flood was worsened by the increased flow of water down the local river (the Eden) from further up-stream, causing the river to burst its banks (Figure 5 illustrates the extent of the floods).

An early consequence of the flooding was the loss of several premises significant to the emergency response, including the police headquarters, the fire service headquarters in Carlisle and the city's Civic Centre, which would otherwise have been used as a reception centre for evacuees. The loss of the police HQ meant the loss of a number of IT systems that would otherwise have been employed in the command and control of the response. In addition, by the morning of the 8th January, electrical power throughout Carlisle had been lost due to the flooding of a critical substation. Mobile cell phone communications were also affected. By late afternoon on the same day, the UHF radio transmitter on the civic centre began to fail as its batteries exhausted.

As a consequence, the Cumbria General Emergency plan was invoked (there was no specific flood plan) and a major incident was declared. Strategic (Gold in UK terminology) and tactical (Silver in UK terminology) commands were established at Penrith police station, and at Carlisle Castle respectively. These locations are approx 30km from each other. The transfer of command and control functions to these alternate premises caused immediate difficulties, since the new IT suite at Penrith had not yet been completed, and Gold command did not have access to relevant local information (maps of Carlisle etc) at their new location.

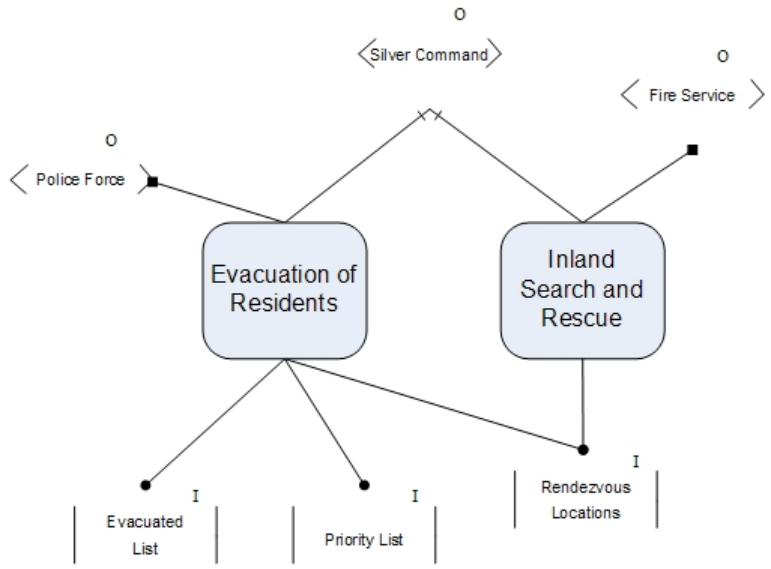
To respond to the emergency, the police established a mobile police station in the city centre and initiated a search and rescue operation in conjunction with the Fire Service in the areas affected by flooding. This included the establishment of rendezvous locations near to the flooded areas. The local Ambulance Service Trust were responsible for transportation of evacuated residents from rendezvous locations to reception centres, as well as supporting medical care in the centres. Boats and RAF helicopters were used to assist in the evacuations. Three reception centres were established for evacuees and provisioned with essentials, including food and emergency generators. In addition to the immediate response, Gold command also coordinated communications with the media in order to distribute information, including advice to evacuate areas of Carlisle where possible.

Following the flooding, the Cumbria County Emergency Planning office revised their preparations and prepared a new plan specifically to respond to flood events [8]. This was a significant amendment of the previous plan which incorporated their experiences of dealing with the flooding emergency.

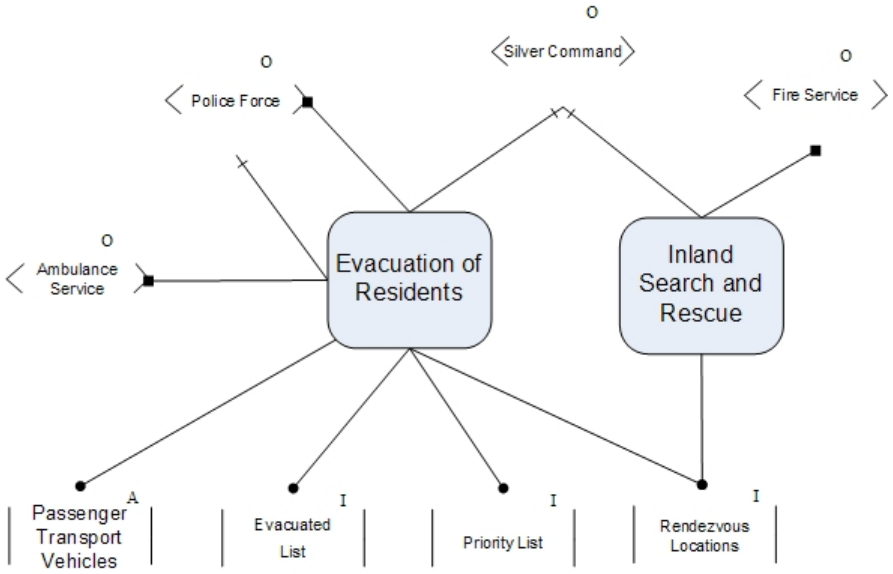
The rest of this section presents a selection of responsibility models with particular reference to the discharge of responsibilities associated with evacuation. The models progress from describing problems which arose during evacuation of residents during the 2005 floods described above, to analysing the specific flood response plans prepared following the evaluation of the response undertaken.

5.2 Evacuation in 2005

As part of the response to the flooding in 2005 described above, the Police Force were responsible to Silver Command for evacuation of residents from areas threatened by flooding, whilst the Fire Service were responsible for search and rescue operations in flooded areas. These two responsibilities are distinct, since evacuation involves moving people who are not in imminent danger to known rendezvous locations and then transporting them from these locations



(a) Planned Responsibilities.



(b) Responsibilities assigned during the response.

Fig. 6. Responsibilities and resources associated with evacuation of flooded areas.

to reception centres; search and rescue involves recovering people who are immediately threatened (residents of areas already flooded, for example), from their homes to these known locations.

Responsibility models can be used as the basis of a discussion of the responsibility structures documented in the contingency plan and the manner in which responsibilities were discharged during the floods in January of 2005. The as-

signment of responsibilities for evacuation anticipated in the Emergency Plan is illustrated in Figure 6(a). In addition, the figure illustrates the information resources (denoted by text between vertical lines and annotated with 'I'), required by the Police Force in order to discharge their responsibility:

Priority List The list of residences that should be evacuated as a priority. These include, for example, nursing homes and residential care homes.

Evacuated List A list of residences that have already been evacuated, either by the police, or by the residents themselves. This list allows the police to avoid visiting every residence and concentrate resources on priorities.

Rendezvous Locations A list of locations where the Fire Service are able to leave rescued residents so that they can be evacuated to reception centres by the police.

We see from Figure 5 (a) that both Evacuation and Search and Rescue require a shared information resource, namely, the list of Rendezvous locations. These are the places where people gather to be transported to the reception centres. One of the benefits of a model is that it allows us to pose general questions which may reveal vulnerabilities. So, when a model reveals that different responsibilities share information, we can ask the following questions:

> What mechanisms exist to ensure that all agents involved have access to the shared information?
> How are changes to the shared information propagated to all responsibilities?

During the response to the flooding, it became apparent that the Police Force required assistance in evacuating residents from rendezvous locations to reception centres. To provide the extra capacity, the Police Force delegated responsibility for assisting in evacuation to the Ambulance Service Trust. Figure 6(b) illustrates the responsibilities regarding evacuation after the delegation.

> "The Trust was requested to supply vehicles to assist in the movement of people from the affected areas although there was confusion regarding a rendezvous point (RVP). Fire and Police requests for vehicles to assist with the evacuation were to addresses that were inaccessible and not to a predetermined RVP." [10, pp68]

The Trust's debrief report suggests that rendezvous locations agreed prior to the flooding were changed, and that alternative locations also became unavailable during the course of the flooding. The report is of interest, since it describes how an agent was assigned a responsibility, but lacked the associated information resources in order to effectively discharge that responsibility. Asking the above questions when responsibilities changed may have highlighted this problem.

Responsibility: Evacuation			
Information	**Guide word**	**Consequence**	**Probability**
Assembly Points	Never	Trust unable to transport evacuees to reception centres. Build up of evacuees at assembly points	Low
	Late	Large build up of evacuees at assembly points.	Medium
	Early	-	-
	Inaccurate	Large build up of evacuees at assembly points. Resources are wasted as transport sent to wrong locations. Possibility of endangering lives by use of unsafe assembly points	High

Fig. 7. HAZOPS analysis of the evacuation list resource.

Figure 6(b) illustrates the information required by the Trust to discharge its responsibility, but does not provide an analysis of the consequences if that information is unavailable or inaccurate. For this purpose, a HAZOPS analysis of information resources can be employed [4,17].

For a HAZOPS analysis, risks associated with information resources are identified using context relevant guide words. The risks are then assessed for consequences for the system should they occur. Applying HAZOPS analysis to models of responsibility provides a means of analysing the information requirements associated with the effective discharge of a responsibility; that is, what does an agent need to know in order to discharge their assigned responsibility? For contingency planning, the analysis provides a means of assessing potential vulnerabilities in planning documents, if for example, an agent has been assigned a responsibility without access to the relevant information. Note that unlike responsibility modelling, the HAZOPS analysis does not identify vulnerabilities documented in the plan. Rather the methodology is used to investigate the consequences of particular aspects of the plan failing, and thus the robustness of the plan as information resources become unreliable.

Figure 7 shows a HAZOPS description of the risks associated with the Rendezvous Locations information resource. The guide words employed in the analysis are never arrives, arrives late, arrives early, and arrives inaccurate. In each case, the probability and consequences of the risk occurring are stated. For example, the risk that the Trust receives inaccurate information results in ambulances being sent to the wrong locations, wasting resources that could be deployed elsewhere. This reflects the situation in which the Trust is not updated on new locations being used by other agents.

5.3 Analysis of Revised Plan

Following the floods in January 2005, a revised flood plan was constructed. Figure 8 illustrates the responsibilities associated with the issue of a flood warning

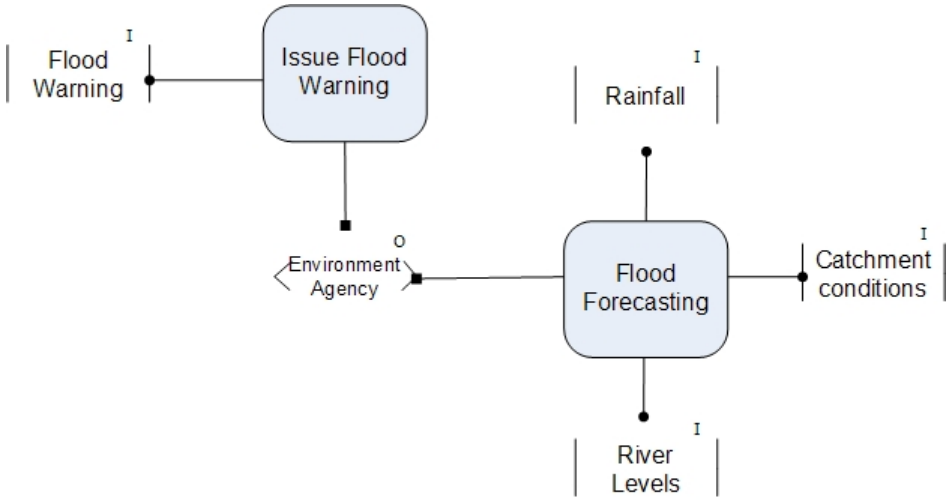


Fig. 8. Responsibilites and associated information resources for flood warning.

by the Environment Agency in the revised plan. The figure illustrates the responsibility of the agency for maintaining a flood watch, with three related information resources (river levels, catchment area status and rainfall). In addition, the agency is responsible for issuing a flood warning when necessary, which has an associated information resource – the flood warning itself.

The responsibility model here shows that issuing a flood warning involves collecting data for flood forecasting then, when appropriate, issuing a flood warning. In this case, we have an example of a situation where the same organisational agent has multiple responsibilities. In such situations, the generic question that we should ask is:

> When an agent holds multiple responsibilities, how are these coordinated and what information must be exchanged?

Figure 9 illustrates the responsibilities of different agencies for evacuation once a flood warning has been issued, and Figure 10 illustrates the same responsibilities with associated information resources. In the plan, responsibility for evacuation and required resources are discussed explicitly. The figure illustrates that in the revised plan command and control are responsible for the initiation of evacuation, based on the advice provided by the Environment Agency of flood warnings and associated risks. Once a decision has been made to evacuate, several agencies are required to coordinate their activities in order to execute an evacuation:

- The police are responsible for the overall coordination of an evacuation and the security of evacuated residences
- The Fire Brigade are responsible for the conduct of search and rescue operations

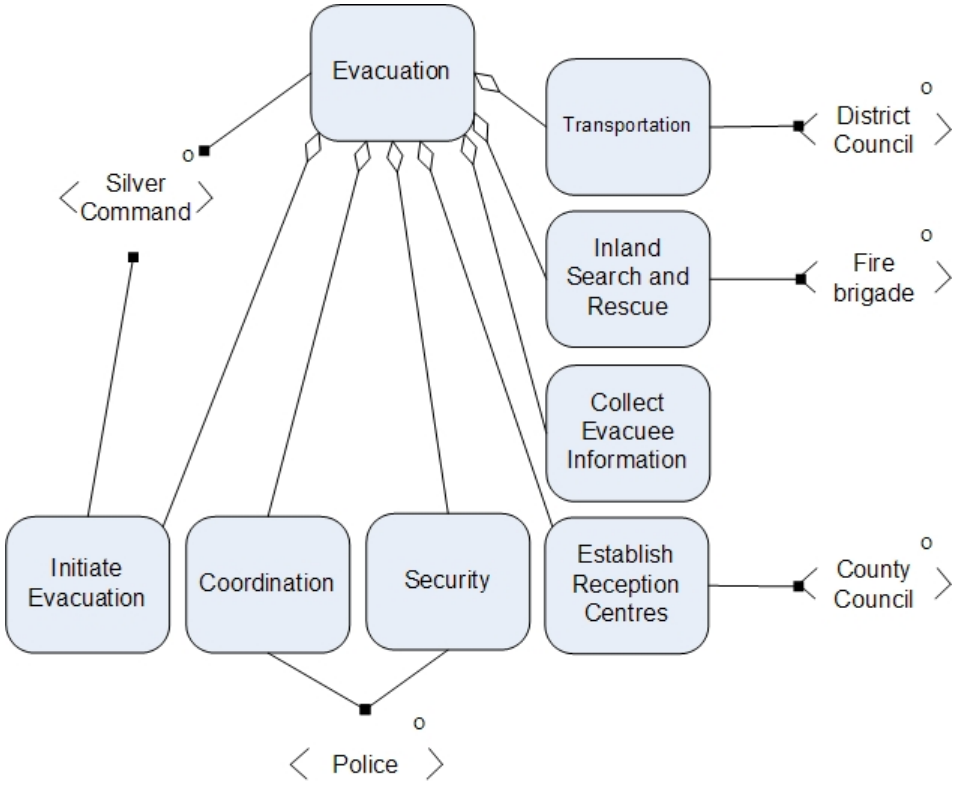


Fig. 9. Evacuation responsibilities

- The County Council is responsible for establishing reception centres during an emergency response
- The District Council are responsible for arranging transport between assembly points and reception centres for evacuees

In addition, a number of information resources are identified explicitly in the plan:

- The list of evacuated residents, collated at reception centres
- The location of assembly points as rendezvous locations between search and rescue operations and transportation to the reception centres

Figure 9 summarises the responsibilities for evacuation as documented in the revised plan. Comparison with the previous arrangement of the responsibilities (Figures 6) illustrates how responsibilities and assignments have changed. In contrast to the approach documented in the debrief report, partially illustrated in Figure 6, a clearer distinction is made between the responsibilities of the police (coordination) and other agencies. In addition, responsibility for transporting evacuees from assembly points is now placed with the District Council, rather than (as in 2005) the Ambulance Service Trust. Responsibility for establishing reception centres has also been modified; in the revised plan, the responsibility is assigned explicitly to the County Council. In addition,

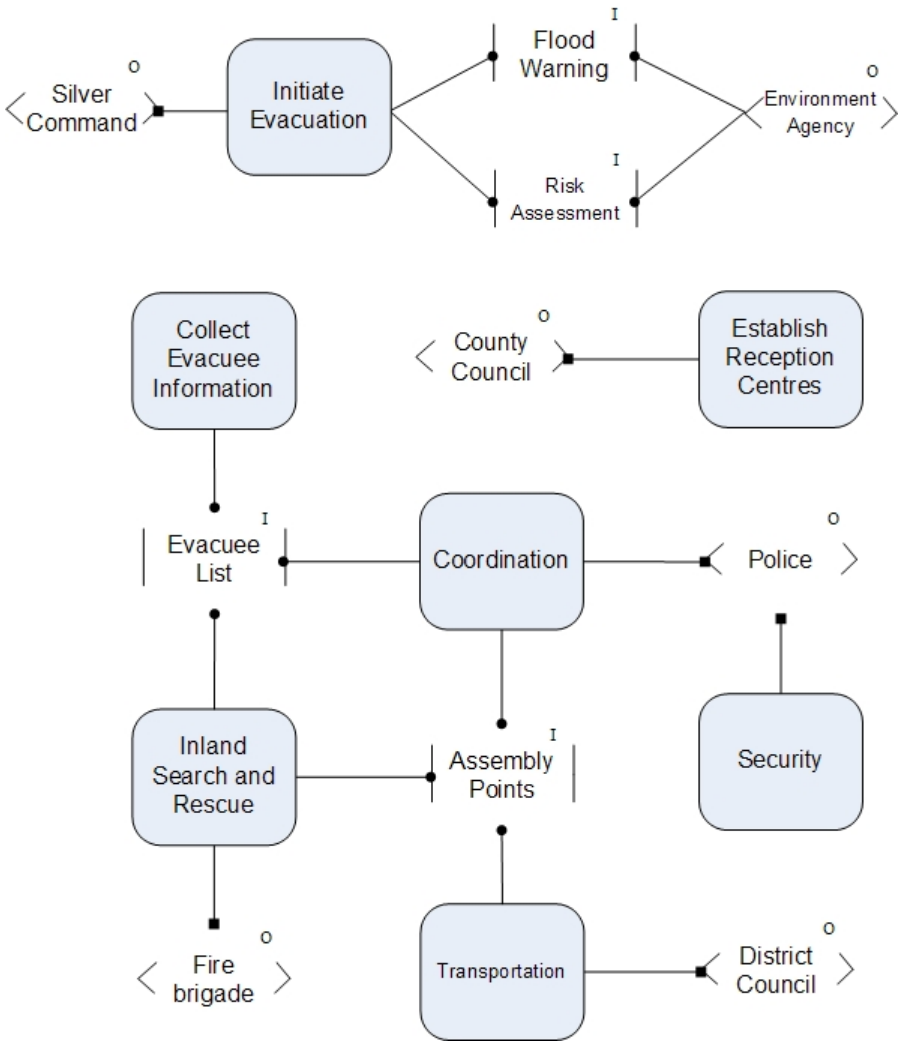


Fig. 10. Evacuation information resources

the description of the responsibility illustrates that the council are responsible for establishing centres *during the response*, in reference to the loss of the anticipated reception centre, the Civic Centre, in the 2005 floods.

Whilst the revised plan documents some of the information resources that will be required during the emergency response, omissions were noted, which could result in vulnerabilities during a flooding response. The responsibility model of the revised flood plan is denoted in Figure 9. What we immediately see from this model, is that there is no agent associated with the responsibility 'Collect Evacuee Information'. This is a classic responsibility vulnerability as described by Sommerville [23] - an unassigned responsibility. Unassigned responsibilities can lead to failure or delay because the other agents in the system cannot or will not take over this responsibility.

Figure 10 extends Figure 9 to show the information resources required to discharge the responsibility. It reveals that the collection of evacuee information

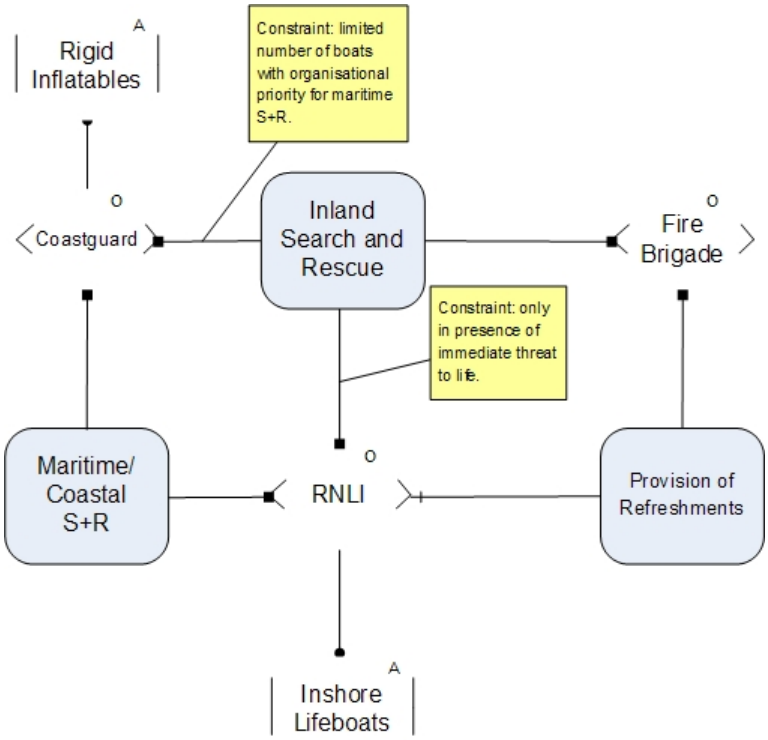


Fig. 11. Coastguard responsibility for inland evacuation (in assistance to the Fire Brigade).

requires a resource which is an evacuee list. Failure to assign a responsibility means that it is unclear who is responsible for compiling this list.

5.4 Coastguard Assistance

During the evacuation caused by floods in 2005, the resources of the Coastguard, normally deployed for coastal or maritime search and rescue operations, were used inland to assist the Fire Brigade with evacuation of flooded areas. This (then ad-hoc) arrangement, is reflected explicitly in the revised plan, and illustrated as a responsibility structure in Figure 11, which illustrates the consequences of constraints for discharge of responsibilities.

Constraints refer to the manner in which a responsibility will normally be discharged by an agency. In addition, the example illustrates how further additional responsibilities may be assigned as a result of an initial responsibility delegation. The example refers to the listing of Coastguard responsibilities in the revised flooding plan and the similar description of responsibilities for the Royal National Lifeboat Institution, a largely voluntary organisation [8, §3 pp3-5].

The figure illustrates that the Fire Brigade are responsible for Inland Search and Rescue, as (for consistency) is stated in Figure 9. The Coastguard and RNLI are both responsible for maritime and coastal search and rescue operations. In addition, the Coastguard and the RNLI may also be responsible for inland search and rescue, but these are subject to constraints. The figure denotes that the Coastguard and RNLI uses their available physical resources (resources annotated by an 'A') to assist in Inland search and rescue. For the Coastguard, the constraint applies to the sharing of suitable boats and crews between the tasks of maritime and inland search and rescue, with maritime search and rescue considered an organisational priority. Thus, the agency may not be able to assist in search and rescue operations resulting from inland flooding when engaged in operations off-shore. Similarly the RNLI may also assist in the discharge of search and rescue responsibilities, subject to the availability of boats for inshore use. The revised flood plan also describes how assistance will only be provided in circumstances where the RNLI organisation judges there to be an immediate threat to life, and may withdraw those resources once the threat has subsided.

In addition, the model shows that, as stated in the emergency plan, RNLI considers the Fire Brigade responsible for provision of refreshments to the RNLI team whilst that organisation assists in search and rescue operations. This illustrates how the assignment of responsibilities to an organisation may result in the further assignment of responsibilities to third parties in order for the responsibility to be discharged. This seems to be a low-level detail but it was quite explicit in the revised flood plan. We suspect there are political reasons for this. Highlighting it in a responsibility model means that its relevance can be discussed by the agents involved.

As for the emergency plan prior to 2005, a HAZOPS analysis may also be undertaken on the identified information resources for responsibility discharge and the consequences for the discharge of responsibilities should particular information resources be unavailable. Note that the HAZOPS analysis in this case is not used to explain the vulnerabilities which caused known failures, rather the analysis provides a (non-expert) indication of potential vulnerabilities in the revised emergency plan.

Figure 12 illustrates a HAZOPS analysis of some of the information resources identified in the revised plan with respect to associated responsibilities. The upper form analyses the consequences of failure with respect to the initiation of an evacuation, identifying the importance of the issue of a flood warning in order to ensure the timeliness of response by the emergency services, and the importance of correct information on flooding events in order to prepare an accurate response.

The lower part of the figure analyses information resources associated with

Responsibility: Initiate Evacuation			
Information	**Guide word**	**Consequence**	**Probability**
Flood Warning	Never	No preparation is made for evacuation	Low
	Late	Preparation occurs later than optimal	Medium
	Early	Prediction later proves inaccurate	Low
	Inaccurate	Incorrect areas are evacuated	Low
Risk Assessment	Never	Decision on evacuation is less informed	Low
	Late	Initiation of evacuation occurs late	Low
	Early	-	-
	Inaccurate	Incorrect decision on evacuation is made	Medium

Responsibility: Coordinate Evacuation			
Information	**Guide word**	**Consequence**	**Probability**
Evacuee List	Never	Evacuation is hard to plan – operation becomes "ad-hoc" as residents are evacuated as they are discovered.	Low
	Late	Initial evacuation is "ad hoc" until information is available.	Low
	Early	-	-
	Inaccurate	Inappropriate resources are allocated to evacuation – causes inefficiencies	Medium
Assembly Points	Never	S+R and Transport cannot be directed to rendezvous .	Low
	Late	Evacuation is delayed as S+R services cannot disc harge evacuees.	Medium
	Early	Assembly points may be changed (due to flooding) so information is incorrect.	Medium
	Inaccurate	S+R and Transport cannot be directed to rendezvous .	Medium

Fig. 12. HAZOPS analysis of the revised evacuation plan information resources.

the coordination of an evacuation (a responsibility assigned to the police). The importance of accurate information on assembly points has already been discussed above, although the analysis is extended here to the potential risk of early distribution of information on assembly points, if this information later becomes inaccurate.

The HAZOPS documentation also analyses risks associated with information concerning evacuees. In particular, accurate and timely information is required on the location and numbers of evacuees within areas at risk of flooding. The revised plan for flooding in Cumbria contains an appendix listing the flood catchment areas and approximate number of residents. However, the approximation is made on a generic multiplier of the number of residencies in the area, which may not be appropriate for small geographic divisions in which large deviations from the mean average may be expected.

5.5 Information Channels

Following the HAZOPS analysis of the information resources required for evacuation, a further responsibility model may be constructed of the communications infrastructure on which information will be communicated. This is necessary as vulnerabilities are not just due to information issues but may also arise because of problems in the communication channels used to transmit and share information.

The use of cellular networks in particular raises a number of issues that need to be outlined in order to identify possible responsibility vulnerabilities. In most emergency operations communications play an important role. Personnel equipped with mobile phones as resources could be affected by constraints including:

(1) Power, both for individual units and for mast relays
(2) Availability of specially equipped handsets in the event of the activation of the "Access Overload Control System" which can, in emergencies filter traffic to allow communication only by enabled handsets
(3) Operation of the existing fixed line system. Subject to power, the mobile network often operates beyond that of the fixed exchanges in flooding situations; however communication with fixed lines would still only be possible if the fixed exchanges were still in service.
(4) Cost implications. Although in actual emergencies these constraints are often relaxed, contingency planning is designed to consider the provisioning of such resources in the long term. This constraint could, for example affect the number of handsets in circulation for emergencies.

We are now working on developing a HAZOPS-style analysis for communication channels in emergency planning. Such an analysis of the communications resources can aid the user in the identification of risks associated with a given resource's state. This is illustrated in Figure 13. We must emphasise here that this represents an early stage for this type of analysis and that we have identified further development of resource hazard analysis as a future area of research.

6 Conclusions and Future Work

This paper has described the potential for applying the notion of modelling responsibility to the task of contingency planning for civil emergencies. The preceding sections have presented three example views of a model of responsibility based on a general contingency plan, flooding incident debrief report and

Responsibility: Communications Provisioning			
Resource(s)	**Guide word**	**Consequence**	**Risk**
Cellular net, fixed wire civilian net, emergency services communications infrastructure	Never	Severe communication problems for all parties involved in the emergency	Low
	Late	Potential to affect early processes of emergency handling	Medium
	Early	Potential cost implications for use of restricted resources. Potential risks relating to the affect of curtailing services to members of the public too soon.	Low
	Insufficient	The need to prioritise resource deployment. The potential for disruption to emergency activity co-ordination	High
	Inappropriate	Potential to affect processes of emergency handling	Low

Fig. 13. HAZOPS of physical resources.

a subsequent revised plan. The examples also illustrate the use of responsibility modelling with HAZOPS information flow analysis to identify information requirements for the discharge of a responsibility and potential vulnerabilities in the event that information delivery fails. This aspect of responsibility modelling can be used to assess the robustness of a contingency plan in the presence of failure.

Our work so far suggests that we can obtain new insights into contingency plans by representing these using responsibility models, and that responsibility and information vulnerabilities can be identified from these models. Our intention is that continuing collaboration with organisations such as the Scottish Environmental Protection Agency (SEPA) will develop the work further. In particular, observations of emergency exercises will provide an opportunity to understand the manner in which contingency plans are executed in response to an incident (this does not necessarily refer to a plan document). In order to facilitate our interactions with collaborating organisations, and to advance and evaluate the research completed so far a CASE tool has been developed to support the construction and analysis of responsibility modelling diagrams. Specific avenues of future research are discussed below:

Analyses of communication channels As discussed, we have started developing an approach to analysing vulnerabilities in communication channels. This is a complex problem as these resources are not simple entities where single guide words can prompt a complete analysis. In our research, we plan to explore how to extend HAZOPS-style analyses for such channels.

Operational responsibility modelling Our current approach to responsibility modelling is based on a static structure of responsibility as expressed in plans. During the operation of complex systems (an actual emergency response for example), responsibilities are dynamic and contingent on local circumstances where an emergency arises. With this approach, resources are analysed as the requirements associated with the discharge of respon-

sibility. An avenue of research we wish to pursue is to examine how responsibility models can be used operationally to support decision making by emergency managers. This will require us to represent the actual rather than the planned allocation of responsibilities and the use of resources as responsibilities are discharged.

Operational responsibility tool support Our existing methodology and tooling is suitable for responsibility planning, but not operation. In order to support access and modification of responsibility models by multiple personnel at different locations, we are developing a mobile responsibility modelling platform, which we plan to evaluate through collaboration with appropriate organisations, including SEPA.

Timeliness One significant omission from the model of responsibility assignment used within these examples is the notion of timely discharge of an agent's responsibility. A desirable extension to the model would be to describe not only the dependencies of an agent, but the time constraints of those dependencies. One potential approach would be the integration of the model of timeliness proposed by Burns et al [3] into the semantics of responsibility assignment described above. Other possible approaches to this area can be seen in the literature for KAOS [9] and i^* [28].

Deontic Logic The similarity between our work on responsibility modelling and the use of deontic logics (logics of norms, obligations and permissions) for system specification by various authors (e.g. [15,26]) was noted in a review of this paper. The methodology described in this paper is intended as a basis for supporting the discussion of responsibilities between relevant stakeholders in a scenario. We are currently investigating the potential benefits of formalising some aspects of the responsibility models constructed in terms of deontic logic, e.g. in providing tool support for identifying more complex responsibility vulnerabilities.

In this paper we advocate that the overall dependability of complex systems that cross organisational boundaries requires us to take a holistic approach to systems engineering. It is not enough to focus on simply improving the dependability of the technical components of the system (hardware and software); it is not even sufficient to extend this with an analysis of individual human factors. Rather, we must also investigate how social and organisational factors influence system dependability and provide some means for systems designers to to analyse and understand these issues. We see our work on responsibility modelling as an attempt to provide engineers with a means of analysing and understanding some of the organisational issues that affect system dependability.

References

[1] Dennis Besnard and Gordon Baxter. Human compensations for undependable systems. Technical Report CS-TR-819, School of Computing Science, Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK, November 2003.

[2] Andrew J.C. Blyth, Jarnail Chudge, John E. Dobson, and M. Ros Strens. ORDIT: A new methodology to assist in the process of eliciting and modelling organisational requirements. In S. Kaplan, editor, *Proceedings on the Conference on Organisational Computing Systems*, pages 216–227, Milpitas, California, USA, 1993. ACM Press.

[3] A. Burns, I.J. Hayes, G. Baxter, and C.J. Fidge. Modelling temporal behaviour in complex socio-technical systems. Technical Report YCS-2005-390, University of York, 2005.

[4] David Bush. Modelling support for early identification of safety requirements: A preliminary investigation. In *Fourth International Workshop on Requirements for High Assurance Systems (RHAS'05 - Paris) Position Papers*, Paris, France, August 2005.

[5] Civil Contingencies Act, 2004. Ch. 36.

[6] Peter Checkland. *Systems Thinking, Systems Practice.* John Wiley & Sons, 1981.

[7] General emergency plan. Cumbria County Council, Arroyo Block, The Castle, Carlisle, CA3 8UR, August 2002.

[8] Cumbria Local Resilience Forum Flooding Sub-group. *Multi Agency Response Plan for Flooding in Cumbria*, July 2007.

[9] Robert Darimont, Emmanuelle Delor, Philippe Massonet, and Axel van Lamsweerde. GRAIL/KAOS: an environment for goal-driven requirements engineering. In W. Richards Adrion, editor, *ICSE'97: Pulling Together, Proceedings of the 19th International Conference on Software Engineering*, pages 612–613, Boston, Massachusetts, USA, May 1997. ACM Press.

[10] Anna-Louise Day. Carlisle storms and associated flooding multi-agency debrief report. UK Resilience, July 2005.

[11] Guy Dewsbury and John Dobson, editors. *Responsibility and Dependable Systems.* Springer-Verlag London Ltd, June 2007.

[12] John Dobson. New security paradigms: what other concepts do we need as well? In *NSPW '92-93: Proceedings on the 1992-1993 workshop on New Security Paradigms*, pages 7–18, Little Compton, Rhode Island, United States, 1993. ACM Press.

[13] John E. Dobson and Ian Sommerville. Roles are responsibility relationships really. DIRC Project Technical Report. Available at `http://www.comp.lancs.ac.uk/computing/resources/IanS/Ian/Research/Papers-PDF/2005-09/RolesAndResponsibilities.pdf`, October 2005.

[14] Emergency preparedness. HM Government, November 2005. Guidance on Part I of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements.

[15] Samit Kholsa and Tom S. E. Maibaum. The prescription and description of state based systems. In Behnam Banieqbal, Howard Barringer, and Amir Pnueli, editors, *Temporal Logic in Specification, Proceedings*, volume 398 of *Lecture Notes in Computer Science*, pages 243–294, Altrincham, UK, 1989. Springer Verlag.

[16] David Martin, Mark Rouncefield, and Wes Sharrock. Complex organisational responsibilities: The ladbroke grove rail inquiry. In Dewsbury and Dobson [11], chapter 4.

[17] John. A. McDermid and David J. Pumfrey. A development of hazard analysis to aid software design. In *Compass'94: 9th Annual Conference on Computer Assurance*, pages 17–26, Gaithersburg, MD, 1994. National Institute of Standards and Technology.

[18] Enid Mumford. The story of socio-technical design: reflections on its successe, failures and potential. *Information Systems Journal*, 16:317–342, 2006.

[19] Sir Michael Pitt. Learning lessons from the 2007 floods. The Pitt Review, Cabinet Office, 22 Whitehall, London SW1A 2WH, December 2007.

[20] E.L. Quarantelli. Disaster crisis management. Preliminary Paper 113, Disaster Research Crisis Center, University of Delaware, 1986.

[21] Denis Smith. For whom the bell tolls: Imagining accidents and the development of crisis simulations in organizations. *Simulation & Gaming*, 35(3):347–362, September 2004.

[22] Denis Smith. Dancing around the mysterious forces of chaos: exploring issues of complexity, knowledge and the management of uncertainty. *Clinician in Management*, 13(3–4):115–123, August 2005.

[23] Ian Sommerville. Models for responsibility assignment. In Dewsbury and Dobson [11], chapter 8.

[24] Tim Storer and Russell Lock. An integrated model of responsibility for the analysis of the dependability of socio-technical systems. Project Working Paper 1, InDeED Project, 2007. `http://www.indeedproject.ac.uk/publications/responsibility-modelling.pdf`.

[25] Ros Strens and John Dobson. How responsibility modelling leads to security requirements. In *NSPW '92-93: Proceedings on the 1992-1993 workshop on New security paradigms*, pages 143–149, New York, NY, USA, 1993. ACM Press.

[26] R.J. Wieringa and J.-J.Ch. Meyer. Actors, actions and initiative in normative system specification. *Annals of Mathematics and Artifical Intelligence*, 7(1-4):289–346, 1993.

[27] Robin Woolven. UK civil defence and nuclear weapons 1953–1959. UK Nuclear History Working Paper 2, Mountbatten Centre for International Studies, December 2006.

[28] Eric S. K. Yu. Agent-oriented modelling: Software versus the world. In Michael Wooldridge, Gerhard Weiß, and Paolo Ciancarini, editors, *AOSE*, volume 2222 of *Lecture Notes in Computer Science*, pages 206–225, Montreal, Canada, May 2002. Springer.